Seguridad en GNU/Linux (I)

SANS: System Administration, Networking and Security Institute.

CERT: Computer Emergency Readiness Team.

RECUERDA:

- Principio de mínimo privilegio.
- Una cadena es tan fuerte como su eslabón más débil.

1. Usuarios y contraseñas

- Usar buenas contraseñas. No permitir contraseñas nulas o débiles (nombres, fechas, ...). Cambiar la clave con cierta frecuencia.
- No abusar de la cuenta de root. Vigilar los sudoers.
- Formar a los usuarios en seguridad informática básica.

2. Comunicaciones

- Vigilar los servicios abiertos. Abrir sólo los estrictamente necesarios.
- Configurar todos los servicios abiertos. No confiar en las instalaciones por defecto.
- Utilizar un firewall local y un firewall de red.
- Usar un sistema de detección de intrusos de red.
- No aceptar correos sin firmar, especialmente si llevan adjuntos. Cuidado con el Phising.
- Cifrar todas las comunicaciones, siempre que sea posible. Usar SSH o IPSEC.
- No usar sistemas inseguros de compartición de ficheros. Especial cuidado con SAMBA (Microsoft SMB).

3. Gestión de datos y software

- Mantener el sistema actualizado.
- Sólo instalar software de fuentes fiables.
- Particionar el disco y vigilar las opciones de montaje de las particiones /tmp y /home.
- Realizar backups periódicos del sistema, especialmente de /etc y /home.
- Vigilar los logs y la actividad del sistema.
- Establecer permisos restrictivos sobre los ficheros y carpetas. Dar el mínimo acceso posible. Usar ACLs si es necesario un control muy fino de los accesos.
- Si se dispone de arranque dual, proteger con antivirus, firewalls, antispyware, ... al Windows. Un virus de Windows podría dañar la partición de Unix / Linux (desde Windows).
- Cifrar los datos personales con criptografía fuerte: gnupg.